iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** IX **Month of publication:** September 2018

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IX, Sep 2018- Available at www.ijraset.com

App Security through Secret Questions

Krati Chauhan[1], Megha Singh[2]
[1, 2]*CIIT, Indore*

Abstract: ***These days we can find many cases of data theft by the intruders for making their own profit by using the hacked data. When talking about different types of attacks on personal data of users and precautions against them, there are many possible ways for both. Manually input passwords are the most commonly used security schemes in daily use applications. It has been scientifically proven that human brain configures a psychologically weak password, as they face problem remembering strong ones, which can easily be guessed by shoulder surfers. Then came the pattern scheme in existence which is the most used security scheme till date for security in smartphone devices. Also the bio-metrics are being used on a large scale level such as banks, defence etc. but when it comes to personal use, it cannot be preferred due to its very high cost. Apps related to networking services (i.e. chatting, social-networking, e-mailing, net-banking etc.) are more prone to attacks as they contain more important information. Secret questions have been widely used by many web applications as the secondary authentication method for resetting the account password when the primary credential is lost. When creating an online account, a user may be required to choose a secret question from a pre-determined list provided by the server, and set answers accordingly. The user can reset his account password by providing the correct answers to the secret questions later. For the ease of setting and memorizing the answers, most secret questions are blank-flings and are created based on the long-term knowledge of a user's personal history that may not change over months/years (e.g., What's the model of your first car?). However, existing research has revealed that such blank-filling questions created upon the users long-term history may lead to poor security and reliability In this paper we present an authentication system called "App Security through Secret Questions" that creates a set of secret questions based on smartphone user's basic application usage, personal details and phone status. We will develop a prototype on Android smartphones and evaluate the security of secret questions by asking them to strangers who would answer the questions by guessing and without the help of online tools.***

Keywords: Memorability, Prevalence, Two-factor authentication, Prototype, Secret Question

I. INTRODUCTION

Now-a-days, use of smartphone apps has been increased. There are some important transaction related apps requires more authentication so that Secondary Authentication Feature is essential for such apps for security concern [2]. Most of the apps need to make registration, which includes set of secret questions based on only personal information, where user has to choose some question and provide answers to selected questions. Those questions are next used for recovery of password. Where correctness of answers are checked for authentication purpose, and only if right user is using it and giving correct answers then only he or she can able to reset or recover password. Through public user profiles, user's personal information can be easily guessable by friends or closers, strangers. These public profiles can be obtained from online social media like face book, twitter or from results of different search engines. This results in loss of reliability. For reliability, user has to memorize correct answers for security questions. User can face difficulty to remember correct answer for each question. So questions are asked based on user's recent smartphone usage. SMS, Location, Call log questions and Calendar event questions are included. Where user only needs to remember short term data related to smartphone usage like 'To whom user recently called', 'To whom he sent SMS', etc. Some questions are based on analysis of log data. These questions are based on duration of calling and frequently made calls. When user lost their primary credentials it is then as a secondary mechanism challenge questions are an increasingly important in such cases. The assumption is that querying for already known information may be more usable than querying specifically memorized information such as passwords. The improved memorability is undeniable when the question is a stereotypical one such as "What is your mother's maiden name?" However, further questions may suffer from usability problems of applicability or repeatability. For example, questions such as "What is your pet's name?" fail to apply to users who have no love of animals; questions such as "What was your first address after leaving home?" may require some kind of changing formats in the answer such that user may answer same question if different ways like "115/6 MG Rd" or "Flat 6, 115 MG Road" [7]. To improve the applicability of the system at least few questions are chosen from the users challenge questions which extend or replace the existing system. It has also been suggested that this allows users to choose more secure questions for which it is difficult to find the answers in publicly available sources.

While users are selecting their own security questions, in such cases we do not know whether user are really trustable. Will they really choose questions which have good usability? From a set of user chosen security challenge questions what kind of security we expecting is a big question. When we forgot password and trying to reset it, the four largest webmail providers – AOL, Google, Microsoft, and Yahoo uses personal (a.k.a. 'secret') questions to authenticate account holders. While other web services may authenticate users who have forgotten their passwords via their email addresses, webmail services cannot always do so; many of their users uses only one webmail account and they usually do not have another email account for backup purpose while resetting the forgotten password. Such users are having many more other services were they had given same email account as backup account for resetting the password. The four major player in webmail ask only one question to reset the account password. Concerns over the security of these questions abound, in part, because webmail is so popular; the top two webmail services each claim a quarter of a billion active users. Public awareness of the potential weaknesses of personal authentication questions reached new heights when Republican vice presidential nominee Sarah Palin's Yahoo! Mail account was compromised via her question [13].

In fact, prior research suggests that a single personal question is not a sufficiently secure authenticator. In two different studies, one in 1990 [2] and another in 1996 [4], participants were asked personal authentication questions and those they were close to – spouses, relatives, friends are were able to guess 33%-39% of challenge questions. Such studies also notified that memorability of questions are weak; participants forgot 20%-22% of their own answers within three months.

II. RELATED WORK

Zviran and Haga studied the security of secret questions for authentication in 1990 [2], which indicated that the answers of 33% questions can be guessed by the "significant others" who were mainly participants' spouses (77%) and close friends (17%). Another similar study was conducted by Podd et al,which revealed a higher rate of successful guessing (39.5%) [5]. A recent study showed that even an open question written by the user himself was still vulnerable to the guessing attacks launched by his acquaintance [4]. The security of secret questions for authentication was studied by Moshe Zviran & William Haga [2], suggested that most challenging questions are answered by usually close friends or spouse, which having very high rate of successful guessing. A recent study showed that even an open question written by the user himself was still vulnerable to the guessing attacks. The use of a cognitive passwords profile can create a dynamic password environment, where a different combination of cognitive items is used at each log-in attempt. Such a combination can consist, for example, of five randomly selected questions out of a set of 20. User authentication through cognitive passwords is an extension of traditional password usage. It suggests the use of fact and opinion-based cognitive data that is known only to the user, as an authentication mechanism. Practical use of cognitive passwords seems also to be relatively simple. This approach imposes only modest demands on a user and requires relatively little computer logic to implement. All that is needed are simple interactive software routines that can handle initial user enrolment and subsequent cue-response exchanges for authentication. Thus, user authentication, using cognitive passwords, merits consideration as a way to get computer security off the memorability and security horns of the password dilemma, without imposing greater burdens on users.

Leakage of information can be done through collecting information from Friends identities, facebook, gmail identities, age or education data and personal identities [11]. Attacker may use different techniques to guess the facebook password like Alternative email, Friends Identities, Age & Education, Phone number, Personal identity. All such details are now a days easily available on our social network. Attacker may spend few time to search all our personal details any may try to break the password recovery to guess the password [8]. Regarding the reliability, a secret question should be memory-wise effortless for users as in [1]. Few users forgot their answers within six months dominant blank-filling secret questions with case sensitive answers require the perfect literally matching to the set answer, which also contributes to its poor reliability. A variety of secondary authentication mechanisms and configurations of those mechanisms exists; each strikes a different balance among the desirable criteria of reliability, security, and efficiency. Many websites uses secondary authentication mechanism such as email-based authentication. However, websites whose accounts have greater value, such as webmail services, should put careful thought into designing secondary authen¬tication systems. Is has been recommend combining multiple mechanisms, enabling the system to adapt to meet the account holder's security and reliability requirements. Authors also recommend regularly refreshing authentica¬tion information, encouraging users to adjust authen¬tication options on the basis of account activity, and designing with compromised accounts in mind. In today's world, large number of smartphones running with Android operating system. As the smartphone use is increases, more amount of sensitive data are stored on their mobile devices [6]. One of the most common control mechanisms for authenticating users of computer based information systems is the use of passwords. However, despite the widespread use of passwords, only little attention has been given to the characteristics of their actual use. Sensitive data stored on smartphones creates many security issues like app security, protection of data on lost or stolen devices.

Smartphone sensors are used to get the data from short-term and long-term usage of smartphones. Through this data security questions are generated [3]. But when we used the smartphones to generate the security questions, we are not found that sensors are so reliable to get accurate data. With users short-term smartphone usage an authentication system with a set of secret questions has been created. The short-term personal history is less likely to be exposed to a stranger or acquaintance, because the rapid variations of an event that a person has experienced within a short term will increase the resilience to guess attacks. it is feasible to combine multiple lightweight (e.g., true-false and/or multiple choice) questions sequentially to lower the success rate for an attacker. The reduction of attacker's success rate depends on how many lightweight questions we want to combine. For example, three lightweight true-false questions will not incur too much user input efforts, but lead to a low success rate of 12.5 percent for a random guessing attacker, which is lower than the hard-to-guess threshold. Mike Just & David Aspinall studid the Personal Choice and Challenge Questions, in which they discuss about the secondary mechanism when primary credentials are lost [7]. Querying for already known information may be more usable than querying specifically memorised information such as passwords. The analysis revealed that many users were given a low security level due to questions that could be clearly identified as not sufficiently secure. Thus, authors suggest that such questions should be avoided altogether (either as administrative choices, or filtered out as user choices), for example: "What colour is your favourite fruit?", and "Favourite musical instrument?" Even further, there appears to be a lack of variety in the types of questions asked. Most questions aligned to administratively generated questions used by financial institutions. In other words, there was a surprising lack of creativity in the user chosen questions we collected. Thus, it remains an open problem as to whether there are more creative questions and answers that could be used by users (in general), whilst providing an improved level of security and usability. To easily recall, most secret questions are blank-fillings (eg., How many total number of apps installed in your smartphone?), and are created based on the long-term knowledge of a user's personal history that may not change over months/years. However, existing research has revealed that such blank-filling questions created upon the user's long-term history may lead to poor security and reliability [4]–[8]. Swapnil Powar and Dr. B. B. Meshram in 2013 did the survey on Android Security Framework [9], in which they had concluded with the permission user grant while installing android app will produce harmful results. Kirin and Lightweight approaches are basically installing time approaches. While installing if users grants some permission unknowingly, on such situations Kirin not proposed any security mechanism for keeping check on the behaviour of application during runtime. Checking dynamic broadcasts was not track by Kirin. Approach of Apex was more fesible than the Kirin and Lightweight. Which continuously check the application behavior at runtime, and on base of policy do not let an application to do something for which permission is not granted to it. For a large amount of users, we have to collect user requirements. Secondly user may grants such permissions unknowingly while installing applications which may produces harmful results. This problem can be solved by the conjunction of Kirin with Apex, by analyzing the constraints and permissions to verify that security rules are not being violated. Arsalaan. F. Rashid et al. proposed a realistic survey about biometric Figure Print Identification [10]. For non-registering the fingerprint in biometric machine most probable causes for loss of finger print pattern by wear and tear (80%), age (8%), physical injuries to fingers (8%), poor body built with anemia (4%). There is difference in fingerprint image quality across age groups, although most pronounced deterioration is found in > 60 age group. Increase in age group usually affect the error rate in biometric identification. Comparing the skin by younger the aging skin is loose and dry which is because aging results in loss of collagen. Human body shows various age related changes over time. Quality of fingerprints directly depends on skin firmness which affects the quality acquired by sensors. Adarsh Singh, Ankit M.Dighraskar, Krutika R. Fulkar ,et al. in 2016 presented a Implementation of Color based Android Shuffling Pattern Lock [12]. Typically the inbuilt features and various locking systems are providing security to the applications in the smartphones, but they are not up to the mark. They are vulnerable to smudge attacks and shoulder surfing, where the passwords can be easily determined. In this paper, we analyzed the problem in the current locking schemes used in the smartphones. Users found hard to remember the color patterns. Xin Jiang et al. in 2018 proposed an analysis and evaluation of the Android application risk behaviour, monitors and records the behaviour of Android applications through the Android sandbox, and uses the information entropy theory to analyse and evaluate the risk behaviour of Android applications. The proposed method by author can provide reference for application store review and also make Android users have a clear assessment of the risks associated with the application. Based on the above methods, author had collected more than 1200 malicious applications and 400 normal applications, calculates the information entropy of both, compares them, and verifies the validity of the method [13].

III.PROPOSED FRAMEWORK

In this paper, we present an Authentication system based on Secret-Question, called "App Security through Secrete Questions", by making use of smartphone data and user's personal data.

With the data of users short-term smartphone usage we planned to create set of secrete questions with we had proposed a user authentication system. A minimum threshold will be set for the users and if the user satisfies the threshold he will be granted access to his personal application.

The proposed system will be divided into several independent modules:-

A. Personal Details

Here the user needs to enter the personal details that were only known by them. For example their star signs, their blood group, favourite colour, parents birth dates etc. These details are stored in database from which the security questions are raised. Since the personal details are converted as security questions it will be difficult for attacker to guess the answer. The data collected here are personalized data and will be hard to guess.

B. Monitor Phone

Next Module is monitoring our mobile phone data in order to increase the security. This process was separated into 3 phases, Application data, Phone status and Battery status. With users short-term smartphone usage a set of secrete questions are created. Most secret questions are blank-fillings and are created based on the long-term knowledge of a user's personal history. The frequently-changing secret questions will be difficult for attackers to guess the answers. We will use the local database to store the results generated after monitoring phone. We will store the result in encrypted format so that we can achieve more security.

C. *User's Personal Application*

Once the user correctly answers the questions more than the threshold limit then only he/she into his personal application which he has secured using our security application. In case the user login fails the application will be locked after a few attempts. If user not able to clear the threshold limits more than 3 attempts, in such cases we close the security app and send sms notification to emergency number which was registered at the time of registration.

The figure below depicts our proposed system.

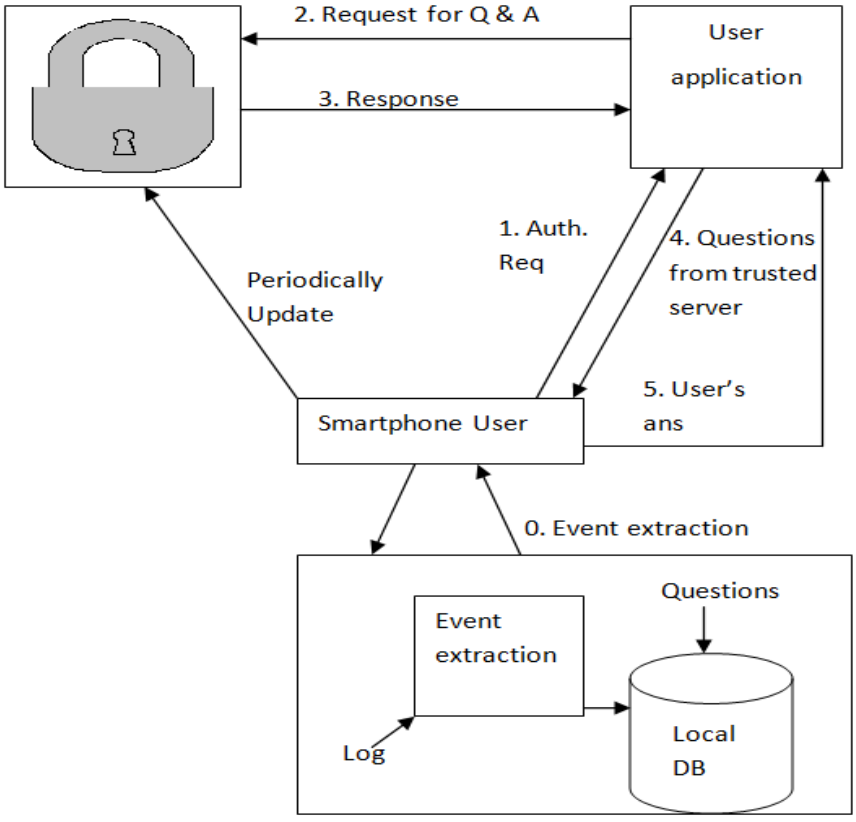


Fig.1. Architecture of Proposed System

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IX, Sep 2018- Available at www.ijraset.com

IV. ALGORITHMIC SOLUTION

First, we present a flow diagram for our system and then show step by step how it works.

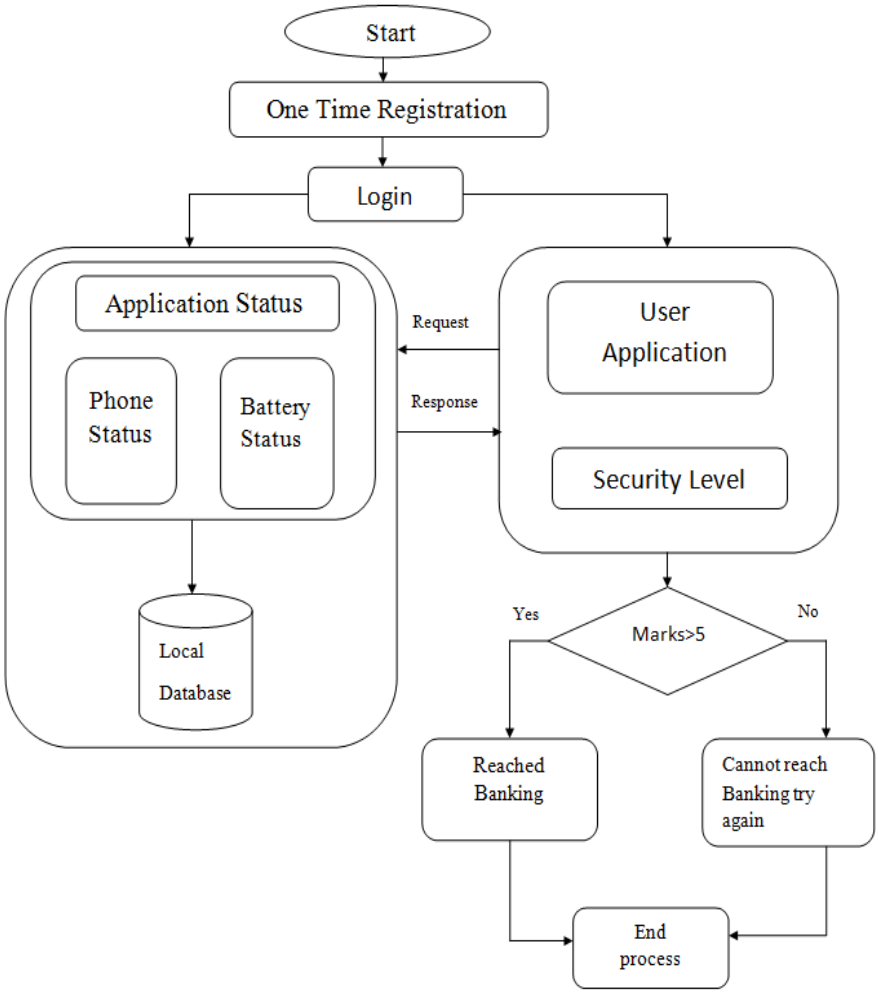


Fig.2. System Flow Diagram

1) *Step 1*: One time registration: In the first step we will create a 4-digit Personal Identification Number (PIN) for the smartphone user. We will also ask for the user's emergency phone number for sending alerts and security question for the recovery process.
2) *Step 2*: Using the generated PIN we will login into our security application.
3) *Step 3*: User needs to fill all personal details like name, date of birth of self and their parents, favorite color, sun sign, etc
4) *Step 4*: Our system will scan the phone status, application status and battery status. Based on this information a set of security questions will be generated and stored in the database.
5) *Step 5*: We will now click on the personal application upon which we have imposed our security application.
6) *Step* 6: Questions will get fired rapidly from the local database.
7) *Step* 7: If the user answers the questions correctly and satisfies the authentication criteria (For example: marks>5 ie. User has to answer minimum 5 questions out of the 7 questions) then user will be granted access to the personal application.
8) *Step 8*: If the user fails to answer the questions correctly more than 3 attempts then the application will stop working and an alert message will be send to emergency number.

V. RESULTS

Proposed system implemented with Eclipse with Android SDK using Java as a basic language. We had installed the app into 18 participants, which are mainly familiar persons as shown in table 1. We also include stranger as we have to check the guessing ratio of the persons who are not known to participants. We have considered following propositions for participants,

Table 1 Participants Selection

Group participants	Relationship to partner participants
< 18 2 (11%)	Spouse 2 (11%)
18–25 5 (28%)	Relative 4 (22%)
26–35 7 (39%)	Friend 6 (33%)
36–55 3 (17%)	Coworker 4 (22%)
55+ 1 (6%)	Other 2 (11%)
(a) Age groups	(b) Relationships

For the analysis purpose we had started noticing the answers given by the 18 participants. We had categorized them into two group's first one which considers the relationship like spouse, friends, etc. and second group which contains the how long participant know each other. We had used to observe the answers for the 10 questions and finding the percentage of guessing. Table 2 and 3 will give a clear idea about our observations.

Table 2. Guesses by participants relationship

Question	Spouse	Relative	Friend	Co-worker	Stranger
What is your blood group?	2/2 (100%)	1/4 (25%)	2/6 (33%)	1/4 (25%)	0/2 (0%)
What is your favorite food?	2/2 (100%)	2/4 (50%)	4/6 (66%)	2/4 (50%)	0/2 (0%)
What is your favorite Color?	1/2 (50%)	2/4 (50%)	5/6 (83%)	2/4 (50%)	0/2 (0%)
Select your star sign	2/2 (100%)	1/4 (25%)	3/6 (50%)	1/4 (25%)	0/2 (0%)
Which type of phone you are using?	1/2 (50%)	1/4 (25%)	5/6 (83%)	2/4 (50%)	0/2 (0%)
What is your current mobile operator?	1/2 (50%)	1/4 (50%)	3/6 (50%)	1/4 (25%)	0/2 (0%)
What is your SIM country code?	2/2 (100%)	4/4 (100%)	6/6 (100%)	4/4 (100%)	2/2 (100%)
Which type of battery is used in your phone?	0/2 (0%)	0/4 (0%)	0/6 (0%)	1/4 (25%)	0/2 (0%)
How many number of application are installed in your mobile phone?	0/2 (0%)	0/4 (0%)	0/6 (0%)	0/4 (0%)	0/2 (0%)
Select target SDK version for chosen app	0/2 (0%)	0/4 (0%)	0/6 (0%)	0/4 (0%)	0/2 (0%)
Total	10/20 (50%)	13/40 (32%)	28/60 (46%)	14/40 (35%)	2/20 (10%)

Fig 4. Guesses by participant's relationship

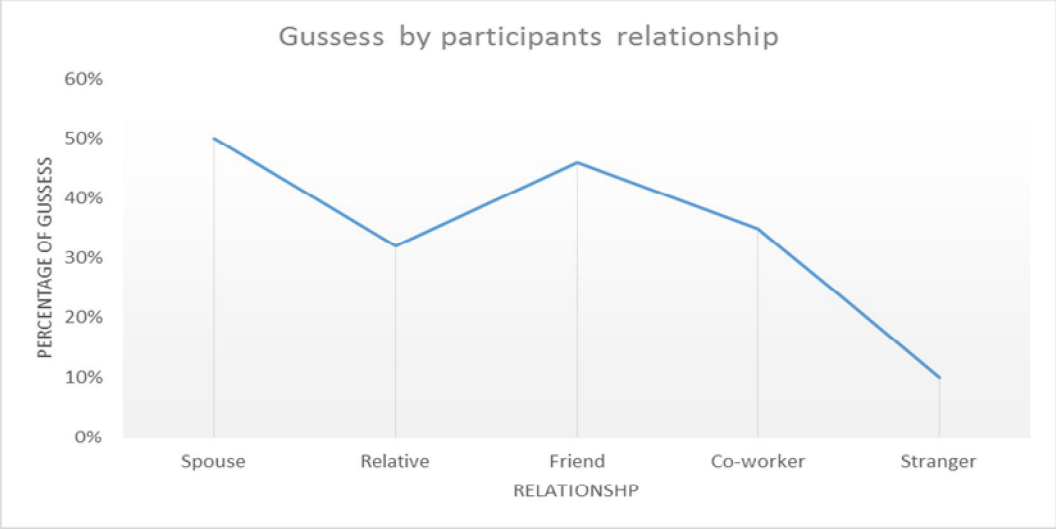
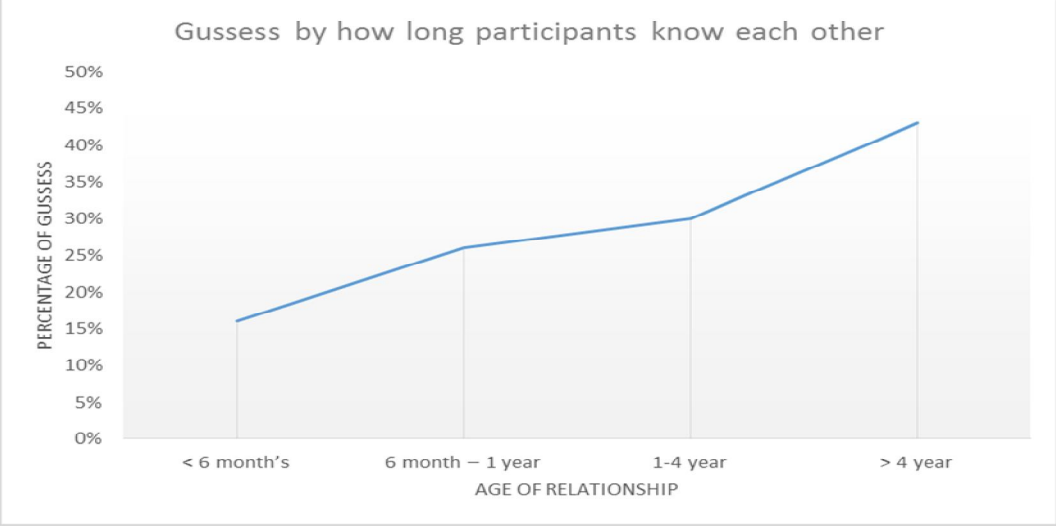


Table 3. Guesses by how long participants know each other

Questions	< 6 month's	6 month – 1 year	1-4 year	> 4 year
What is your blood group?	0/3 (0%)	1/5 (20%)	1/7 (14%)	1/3 (33%)
What is your favorite food?	1/3 (33%)	2/5 (40%)	3/7 (42%)	2/3 (66%)
What is your favorite Color?	1/3 (33%)	1/5 (20%)	2/7 (28%)	2/3 (66%)
Select your star sign	0/3 (0%)	1/5 (20%)	2/7 (28%)	1/3 (33%)
Which type of phone you are using?	0/3 (0%)	2/5 (40%)	3/7 (42%)	1/3 (33%)
What is your current mobile operator?	0/3 (0%)	1/5 (20%)	3/7 (42%)	2/3 (66%)
What is your SIM country code?	3/3 (100%)	5/5 (100%)	7/7 (100%)	3/3 (100%)
Which type of battery is used in your phone?	0/3 (0%)	0/5 (0%)	0/7 (0%)	1/3 (33%)
How much number of applications is installed in your mobile phone?	0/3 (0%)	0/5 (0%)	0/7 (0%)	0/3 (0%)
Select target SDK version for chosen app	0/3 (0%)	0/5 (0%)	0/7 (0%)	0/3 (0%)
Total	2/30 (16%)	13/50 (26%)	21/70 (30%)	13/30 (43%)

Fig 5. Guesses by how long participants know each other



From the two different observations we had come to know that participants who are very close still not able to predict all questions not even participants with more than 4 years of togetherness. As figure 4 and 5 shows the percentage of guessing by different participants.. Participants usually guess the answers about questions which are personal like favorite color, favorite food, star sign, etc but not able to guess answers for how many app installed in the mobile phone. Not even spouse or best friend with more than 4 year in relationship can able to predict the answer for the questions.

This survey shows that it is really hard to guess the answers for the questions generated through our usage of smartphone.

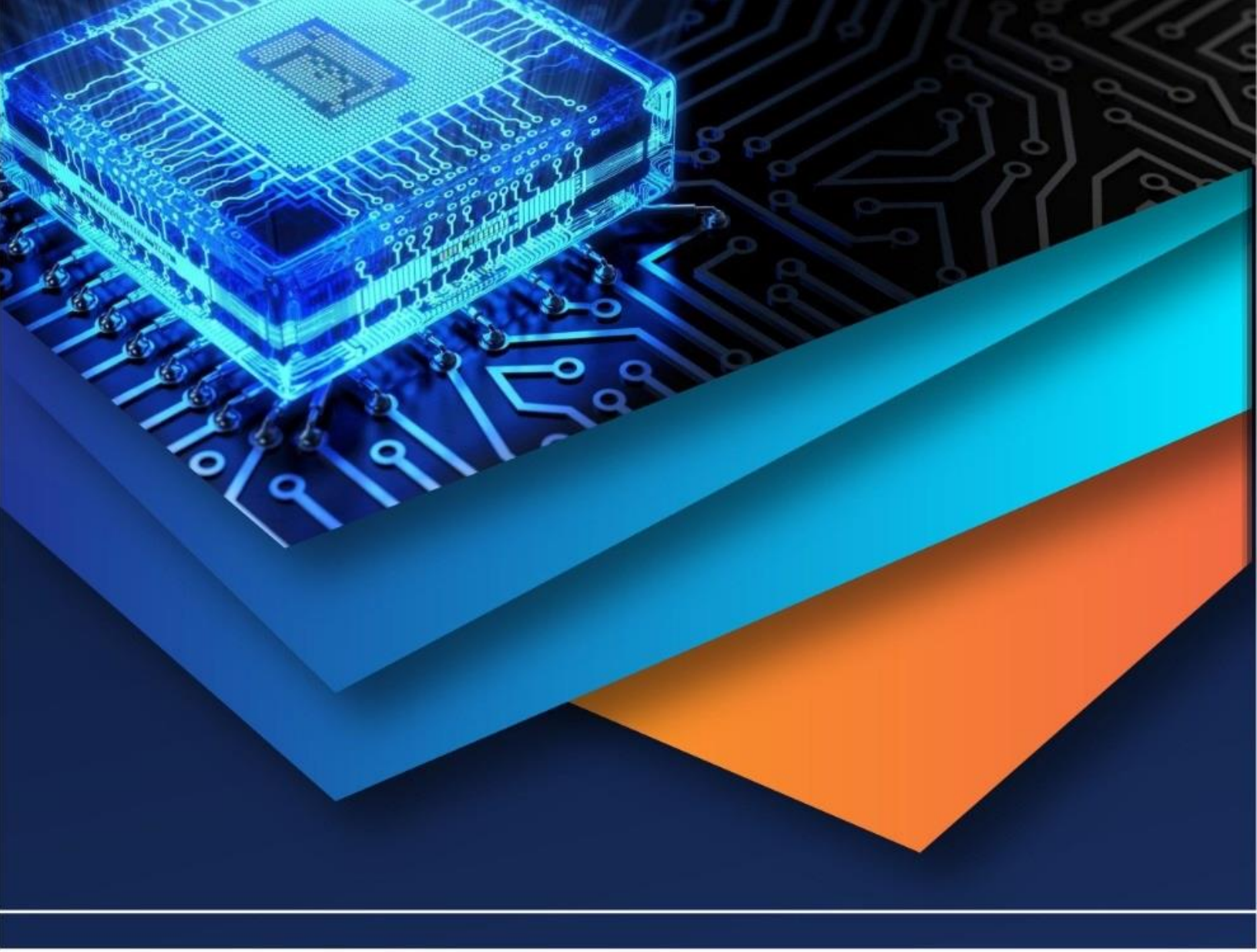
VI. CONCLUSIONS

With our models and analysis, we hope to provide a clearer manifest as to the security and usability offered with challenging question authentication. In particular, the Security Model we have introduced indicates that while individual questions typically provide very limited security, and there exist numerous individual questions that are themselves insecure, there are choices around which a secure system can be built. Though there might be some optimism for more secure questions, usability remains a challenge.

We will in future extend our work on large scale and on diverse populations over a longer time to see the memorability of the users and see the pattern how other guess answers.

REFERENCES

[1] R. Reeder and S. Schechter, When the password doesnt work: Secondary authentication for websites, S and P., IEEE, vol. 9, no. 2, pp. 4349, March 2011.
[2] M. Zviran and W. J. Haga, User authentication by cognitive passwords: an empirical assessment, in Information Technology, 1990.Next Decade in Information Technology, Proceedings of the 5th Jerusalem Conference on IEEE, 1990, pp. 137144.
[3] Peng Zhao, Kaigui Bian, Tong Zhao, Understanding Smartphone Sensor and App Data for Enhancing the Security of Secret Questions, IEEE Transactions on Mobile Computing ,24 March 2016.
[4] J. Podd, J. Bunnell, and R. Henderson, Cost-effective computer security: Cognitive and associative passwords, in Computer-Human Interaction, 1996. Proceedings., Sixth Australian Conference on. IEEE, 1996, pp. 304305.
[5] S. Schechter, A. B. Brush, and S. Egelman, Its no secret. measuring the security and reliability of authentication via secret questions, in S & P., IEEE, 2009, pp. 375390.
[6] S. Schechter, C. Herley, and M. Mitzenmacher, Popularity is everything: A new approach to protecting passwords from statistical-guessing attacks, in USENIX Hot topics in security, 2010, pp. 18.
[7] D. A. Mike Just, Personal choice and challenge questions: A security and usability assessment, in SOUPS., 2009.
[8] A. Rabkin, Personal knowledge questions for fallback authentication: Security questions in the era of facebook, in SOUPS. ACM, 2008, pp. 1323.39.
[9] Swapnil Powar, Dr. B. B. Meshram, Survey on Android Security Framework, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 3, Issue 2" March -April 2013, pp.907-911.
[10] Arsalaan. F. Rashid, Mehreen Lateef, Balbir Kaur, O. P. Aggarwal, Sajad Hamid, Neeraj Gupta, Biometric Finger Print Identifcation Is It a Reliable Tool or Not?",J Indian Acad Forensic Med. April-June 2013, Vol. 35, No. 2.
[11] Mordechai Guri, Eyal Shemer, Dov Shirtz, Yuval Elovici, "Personal Information Leakage during Password Recovery of Internet Services", 2016 European Intelligence and Security Informatics Conference (EISIC), March 2017.
[12] Adarsh Singh1, Ankit M. Dighraskar, et al. "Color based android shuffling pattern lock", International Research Journal of Engineering and Technology, Feb-2016, Vol. 3, No. 2, pp.948-950.
[13] Xin Jiang, Mingzhe Liu, et al. "A Security Sandbox Approach of Android Based onHook Mechanism", Security and Communication Networks, Volume 2018.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY